Detección no autorizada en redes inalámbricas unificadas

Contenido

Introducción

Las redes inalámbricas amplían las redes alámbricas y aumentan la productividad de los trabajadores y el acceso a la información. Sin embargo, una red inalámbrica no autorizada representa un problema de seguridad añadido. Se pone menos cuidado en la seguridad de los puertos de las redes alámbricas, y las redes inalámbricas son una extensión fácil de las redes alámbricas. Por lo tanto, un empleado que traiga su propio punto de acceso de Cisco (AP) a una red inalámbrica o una infraestructura cableada bien protegida y permita el acceso de usuarios no autorizados a esta en principio red protegida puede comprometer fácilmente una red segura.

La detección no autorizada permite al administrador de la red supervisar y eliminar este problema de seguridad. La arquitectura Cisco Unified Network ofrece dos métodos de detección no autorizada que permiten una solución completa de identificación y contención sin necesidad de herramientas y redes superpuestas costosas y difíciles de justificar.

Descripción general de características

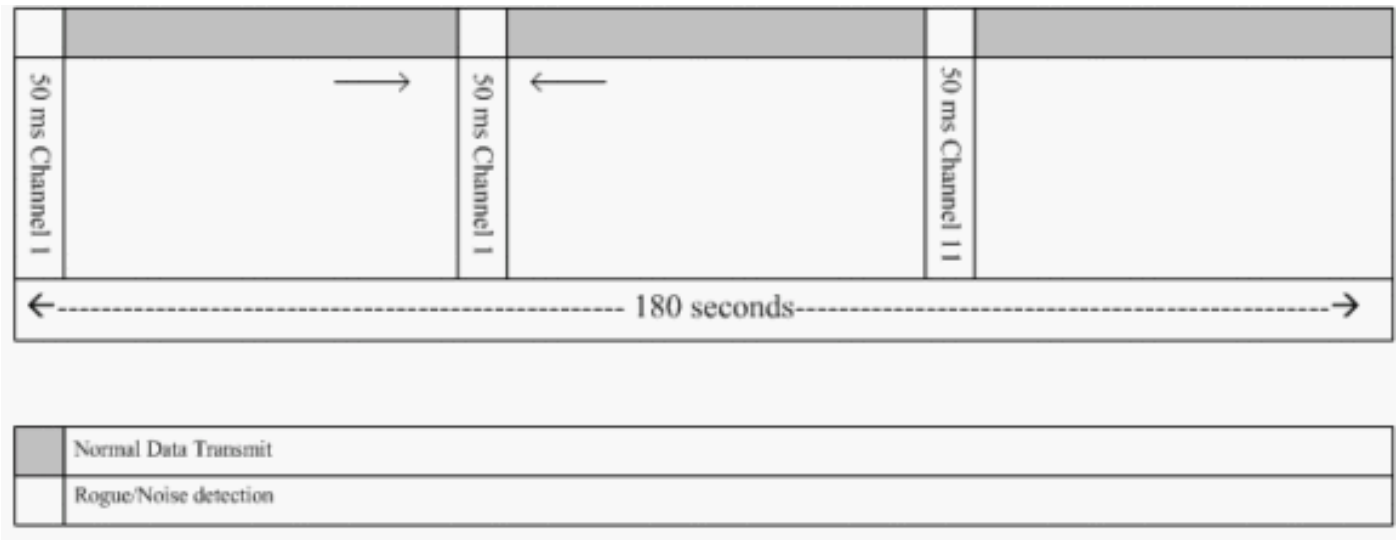
La detección no autorizada no está sujeta a ninguna normativa y no se requiere ningún cumplimiento legal para su funcionamiento. Sin embargo, la contención poco ortodoxa suele plantear problemas legales que pueden incomodar al proveedor de infraestructura si se le deja funcionar automáticamente. Cisco es extremadamente sensible a estos problemas y proporciona estas soluciones. Cada controlador se configura con un nombre de grupo de RF.Una vez que un AP ligero se registra con un controlador, incorpora un **elemento de información de autenticación (IE)** que es específico del grupo de RF configurado en el controlador en todas sus tramas de respuesta de balizas/sonda. Cuando el Lightweight AP escucha tramas de respuesta de balizas/sonda de un AP ya sea sin este **IE** o con **IE incorrecto**, entonces el Lightweight AP informa que AP como un rogue, registra su BSSID en una tabla rogue y envía la tabla al controlador. Existen

dos métodos, a saber, el Protocolo de detección de ubicación no autorizada (RLDP) y el funcionamiento pasivo, que se explican en detalle; vea la sección Determinar cuáles son las Rogues Activas.

Descubrimiento de infraestructura

La detección poco ortodoxa en un entorno inalámbrico activo puede resultar costosa. Este proceso solicita al AP en servicio (o modo local) que cese el servicio, escuche el ruido y realice la detección de rogue. El administrador de la red configura los canales para escanear y el período de tiempo en el que se escanean todas las estaciones. El AP escucha 50 ms para las balizas de cliente no autorizadas y luego vuelve al canal configurado para atender a los clientes de nuevo. Este escaneo activo, combinado con los mensajes vecinos, identifica qué AP son no deseados y qué AP son válidos y forman parte de la red. Para configurar los canales escaneados y el período de tiempo de escaneo, navegue hasta **Wireless > 802.11b/g Network** (bien "**b/g**" o bien "**a**" según el requisito de red) y seleccione el **botón Auto RF** en la esquina superior derecha de la ventana del navegador.

Puede desplazarse hacia abajo hasta **Ruido/Interferencia/Canales de Monitoreo Desconocidos** para configurar los canales a ser escaneados para los rogues y el ruido. Las opciones disponibles son: Todos los canales (del 1 al 14), los canales de países (del 1 al 11) o los canales de asociaciones de canales dinámicos (DCA) (de forma predeterminada, 1, 6 y 11). El período de tiempo de escaneo a través de estos canales se puede configurar en la misma ventana, bajo **Intervalos de monitor (60 a 3600 segundos)** junto con el intervalo de medición del ruido. De forma predeterminada, el intervalo de escucha para el ruido fuera del canal y los rogues es de 180 segundos. Esto significa que cada canal se escanea cada 180 segundos. Este es un ejemplo de los canales DCA que se escanean cada 180 segundos:



Como se ilustra, un alto número de canales configurados para ser escaneados en combinación con los cortos intervalos de escaneo, deja menos tiempo para que el AP realmente preste servicio a los clientes de datos.

El Lightweight AP espera para etiquetar a los clientes y AP como rogues porque estos rogues posiblemente no son informados por otro AP hasta que se complete otro ciclo. El mismo AP se traslada al mismo canal nuevamente para monitorear los APs y clientes no autorizados, así como el ruido y la interferencia. Si se detectan los mismos clientes y/o puntos de acceso, se enumeran como rogues en el controlador otra vez. El controlador comienza ahora a determinar si estos rogues están conectados a la red local o simplemente a un AP vecino. En cualquier caso, un AP

que no forma parte de la red inalámbrica local administrada se considera un rogue.

Detalles de Rogue

Un AP ligero sale del canal durante 50 ms para escuchar a los clientes no autorizados, monitorear el ruido y la interferencia del canal. Cualquier cliente o AP rogue detectado se envía al controlador, que recopila esta información:

- La dirección MAC de punto de acceso no autorizado
- El nombre de AP rogue
- La dirección MAC de los clientes conectados no autorizados
- Si las tramas están protegidas con WPA o WEP
- El preámbulo
- Relación señal-ruido (SNR)
- Indicador de potencia de la señal del receptor (RSSI)

Punto de acceso del detector de rogue

Puede hacer que un AP funcione como un detector no autorizado, lo que le permite colocarlo en un puerto trunk para que pueda oír todas las VLAN conectadas por cable. Continúa buscando el cliente en la subred cableada en todas las VLAN. El AP detector de rogue escucha los paquetes del protocolo de resolución de direcciones (ARP) para determinar las direcciones de capa 2 de los clientes rogue identificados o los AP rogue enviados por el controlador. Si se encuentra una dirección de Capa 2 que coincide, el controlador genera una alarma que identifica el AP o cliente no autorizado como una amenaza. Esta alarma indica que se vio el rogue en la red por cable.

Determinación de Rogues Activos

Los AP rogue deben ser "vistos" dos veces antes de que el controlador los agregue como rogue. Los AP rogue no se consideran una amenaza si no están conectados al segmento cableado de la red corporativa. Para determinar si el delincuente está activo, se utilizan varios enfoques. Entre esos enfoques se incluye el PDL.

Protocolo de detección de ubicación no autorizada (RLDP)

RLDP es un enfoque activo, que se utiliza cuando el AP rogue no tiene ninguna autenticación (autenticación abierta) configurada. Este modo, que está inhabilitado de forma predeterminada, indica a un AP activo que se mueva al canal no autorizado y se conecte al rogue como cliente. Durante este tiempo, el AP activo envía mensajes de desautenticación a todos los clientes conectados y luego apaga la interfaz de radio. Luego, se asociará al AP rogue como cliente.

A continuación, el AP intenta obtener una dirección IP del AP no autorizado y reenvía un paquete UDP (protocolo de datagramas de usuario) (puerto 6352) que contiene el AP local y la información de conexión no autorizada al controlador a través del AP no autorizado. Si el controlador recibe este paquete, la alarma se configura para notificar al administrador de la red que se descubrió un AP rogue en la red cableada con la función RLDP.

Nota: Use el comando **debug dot11 rldp enable** para verificar si el Lightweight AP se asocia y recibe una dirección DHCP del AP rogue. Este comando también muestra el paquete UDP enviado por el Lightweight AP al controlador.

Aquí se muestra una muestra de un paquete UDP (puerto de destino 6352) enviado por el Lightweight AP:

```
0020 0a 01 01 0d 0a 01 .......(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
000...x......... 0040 00 00 00 00 00 00 00 00 00 00
```

Los primeros 5 bytes de los datos contienen la dirección DHCP dada al modo local AP por el AP rogue. Los siguientes 5 bytes son la dirección IP del controlador, seguidos de 6 bytes que representan la dirección MAC de AP rogue. Luego, hay 18 bytes de ceros.

Operación pasiva:

Este enfoque se utiliza cuando el AP rogue tiene alguna forma de autenticación, ya sea WEP o WPA. Cuando una forma de autenticación se configura en AP rogue, el AP ligero no puede asociarse porque no conoce la clave configurada en el AP rogue. El proceso comienza con el controlador cuando pasa en la lista de direcciones MAC del cliente no autorizado a un AP configurado como detector no autorizado. El detector no autorizado explora todas las subredes conectadas y configuradas para las solicitudes ARP, y ARP busca una dirección de Capa 2 coincidente. Si se detecta una coincidencia, el controlador notifica al administrador de la red que se ha detectado un rogue en la subred con cables.

Contención de Rogue activa

Una vez que se detecta un cliente no autorizado en la red por cable, el administrador de la red puede contener tanto el AP no autorizado como los clientes no autorizados. Esto se puede lograr porque los paquetes de desautenticación 802.11 se envían a los clientes que están asociados a APs no autorizados de modo que se mitigue la amenaza que tal agujero crea. Cada vez que se intenta contener el AP rogue, se utiliza casi el 15% del recurso del AP ligero. Por lo tanto, se sugiere ubicar físicamente y quitar el AP rogue una vez que esté contenido.

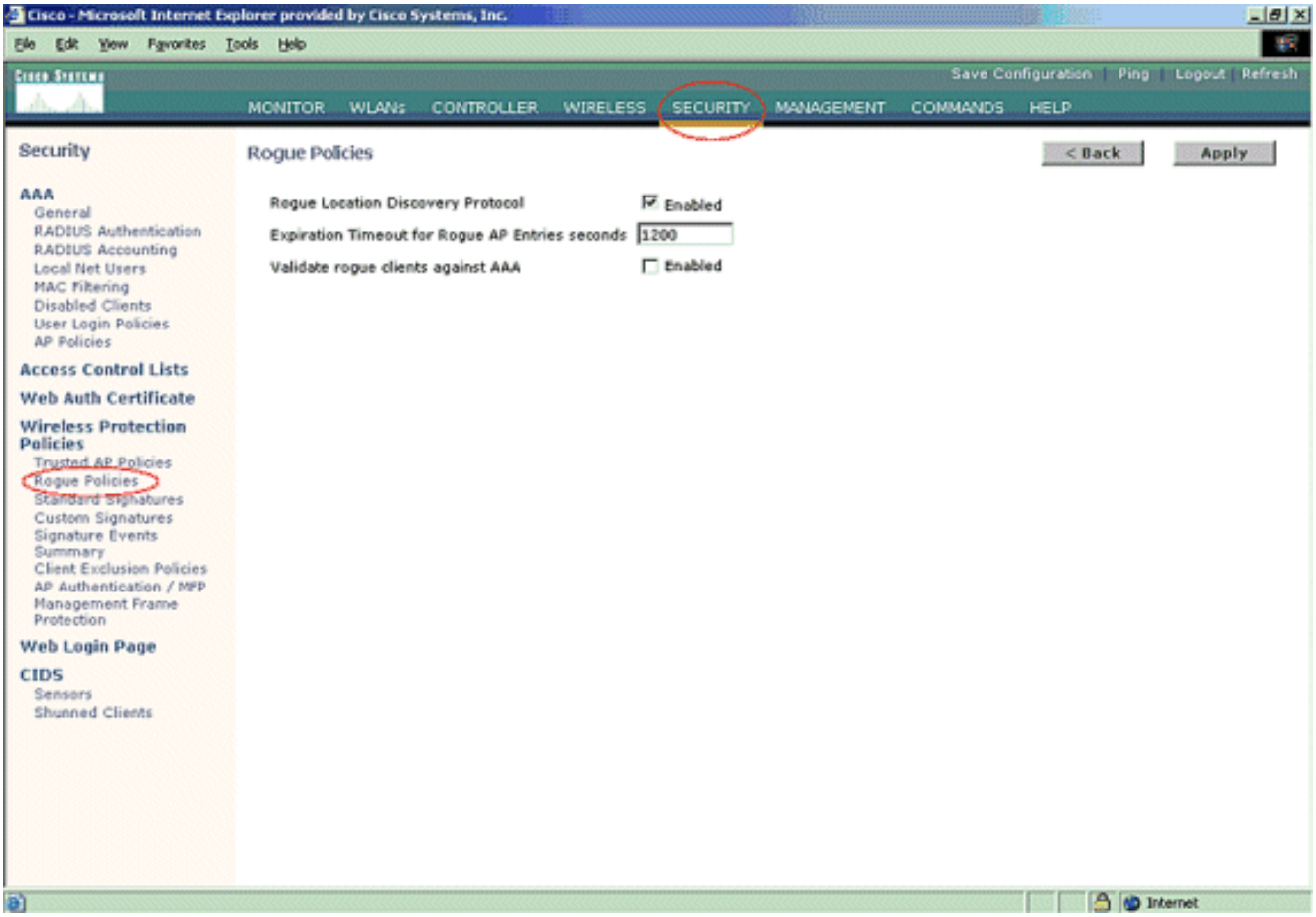
Nota: Desde la versión 5.2.157.0 del WLC, una vez que se detecta el router ahora puede elegir contener manualmente o automáticamente el rogue detectado. En las versiones de software del controlador anteriores a 5.2.157.0, la contención manual es la única opción.

Detección de Rogue: Pasos de Configuración

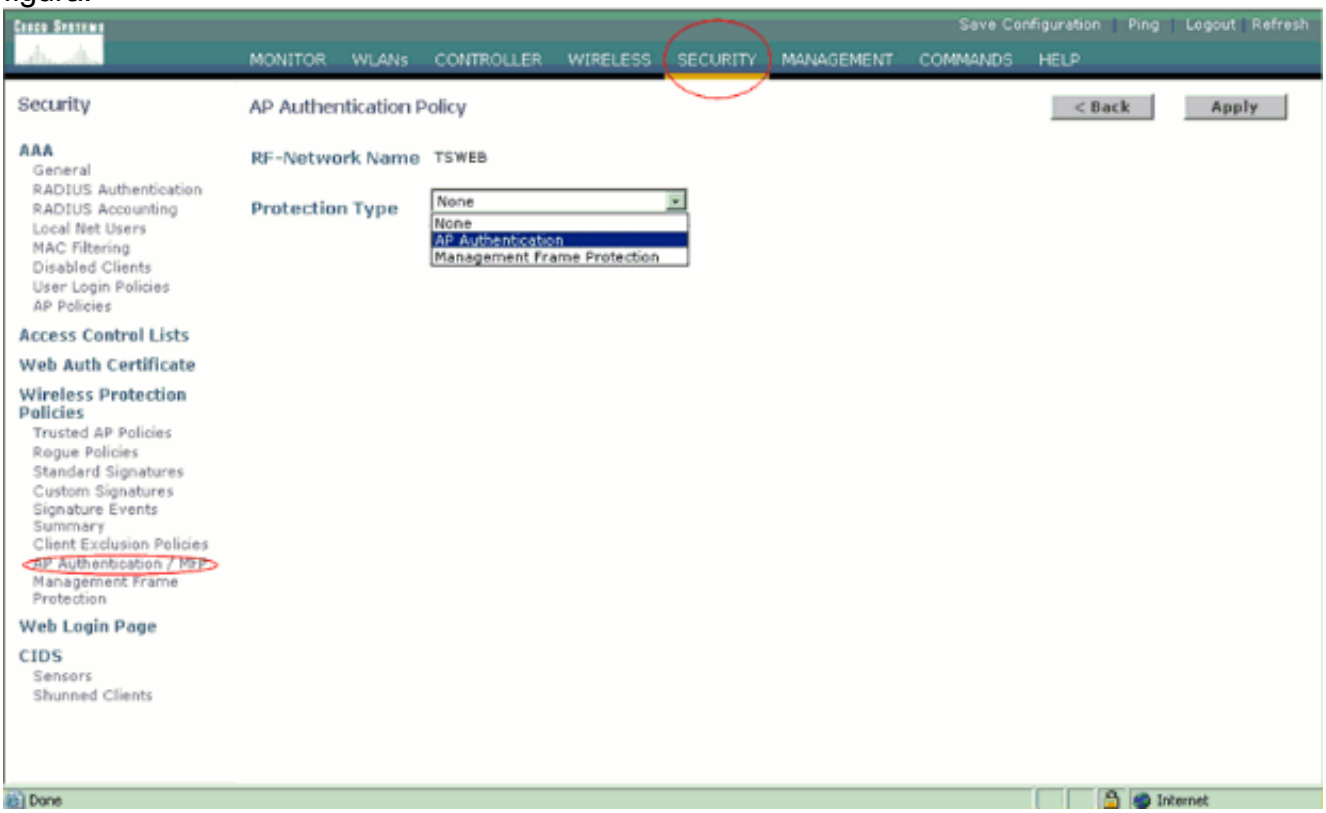
Casi toda la configuración de detección no autorizada se habilita de forma predeterminada para permitir una seguridad de red maximizada y inmediata. Estos pasos de configuración asumen que no se configura ninguna detección de rogue en el controlador para aclarar información importante de detección de rogue.

Para configurar la detección de rogue, complete estos pasos:

1. Asegúrese de que el protocolo Rogue Location Discovery esté activado. Para activarlo, elija **Security > Rogue Policies** y haga clic en **Enabled** en el **Rogue Location Discovery Protocol** , como se muestra en la figura.**Nota:** Si un AP rogue no se escucha durante un cierto tiempo, se elimina del controlador. Este es el **Tiempo de Espera de Vencimiento** para un AP no autorizado, que se configura debajo de la opción
RLDP.

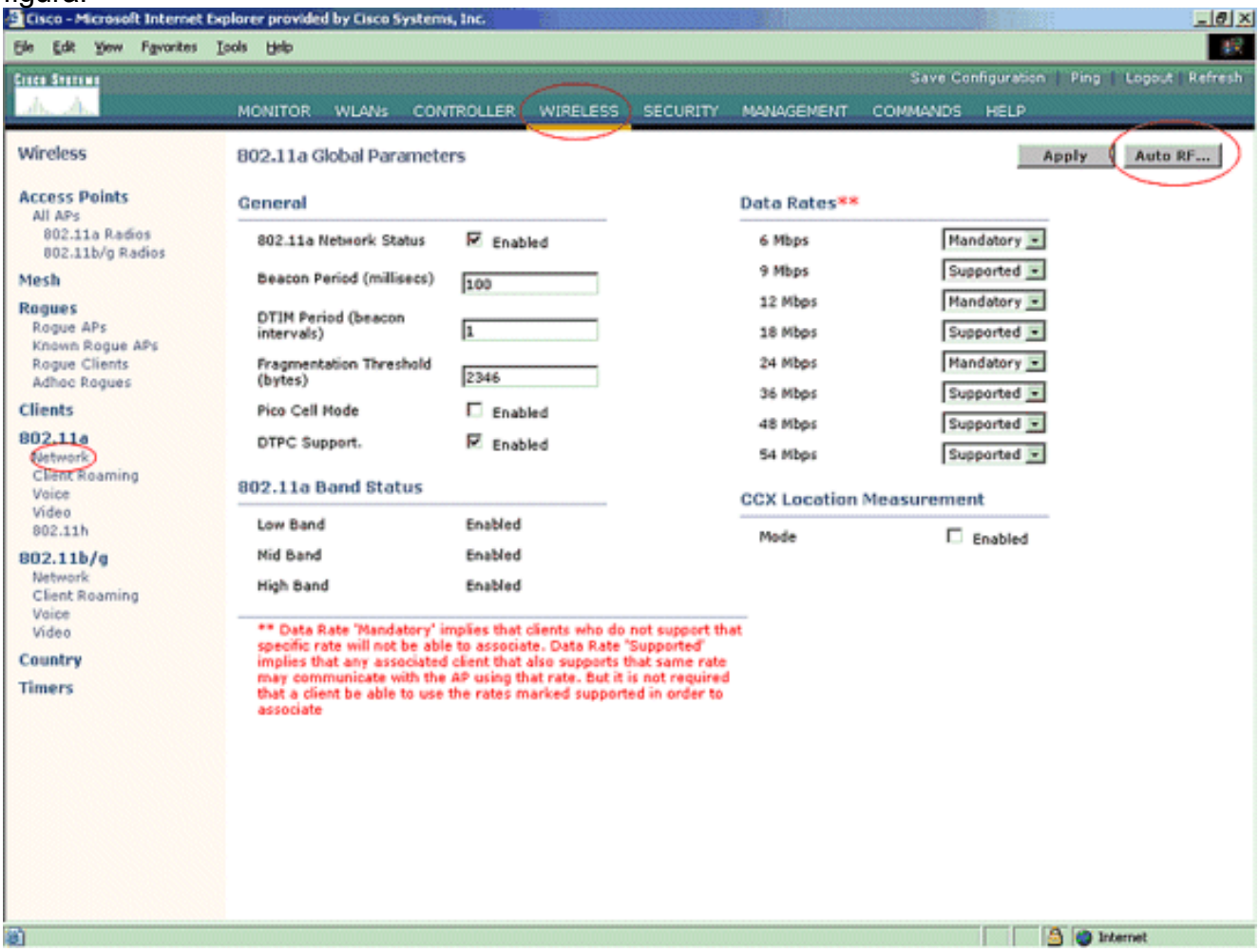


2. Este es un paso opcional. Cuando se habilita esta función, los AP que envían paquetes vecinos RRM con diferentes nombres de **grupo RF** se informan como rogues. Esto le ayudará a estudiar su entorno de RF. Para habilitarlo, elija **Security-> AP Authentication**. Luego, elija **AP Authentication** como Protection Type como se muestra en la figura.

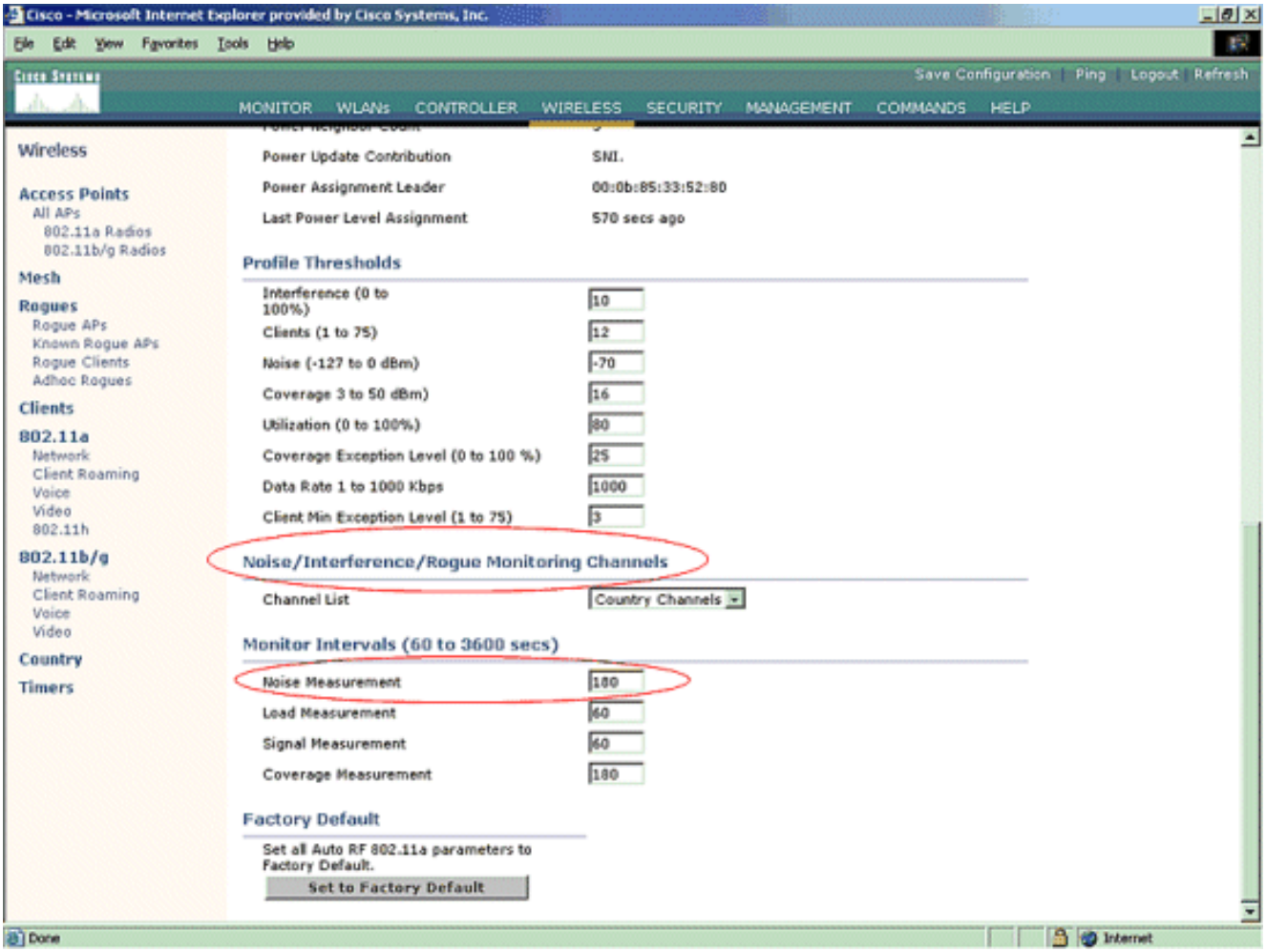


3. Verifique los canales a analizar en estos pasos:Seleccione **Wireless > 802.11a Network** y, a continuación, **Auto RF** en el lado derecho como se muestra en la

figura.



En la página **Auto RF**, desplácese hacia abajo y elija **Ruido/Interferencia/Rogue Monitoring Channels**.



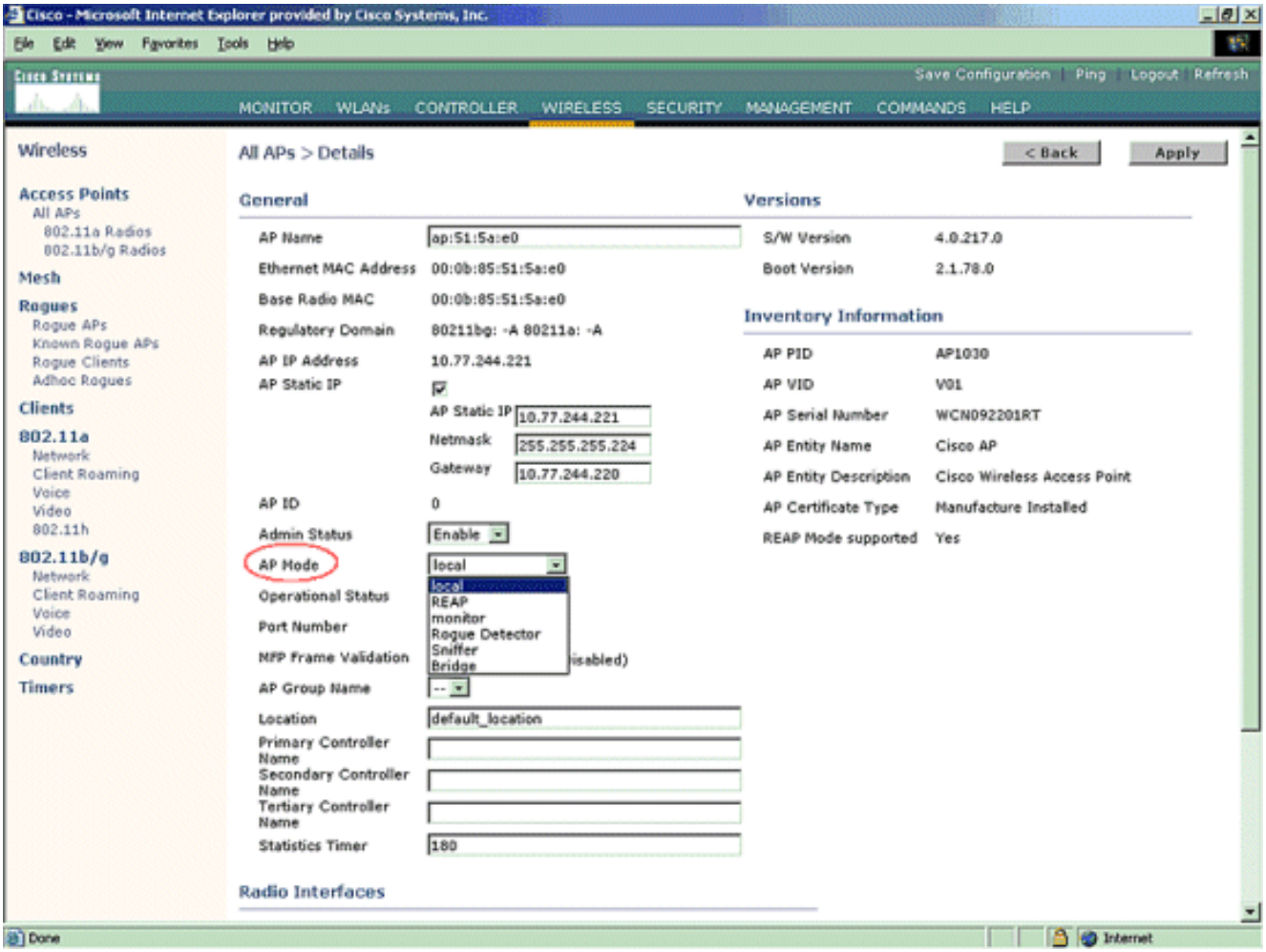
La Lista de canales detalla los canales que se escanearán para el monitoreo de rogue, además de otras funciones de controlador y AP. Consulte Preguntas Frecuentes sobre Lightweight Access Point para obtener más información sobre los AP ligeros y Preguntas Frecuentes sobre Troubleshooting de Wireless LAN Controller (WLC) para obtener más información sobre los controladores inalámbricos.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Establecer el periodo de tiempo para analizar los canales seleccionados:La duración del escaneo del grupo de canales definido se configura bajo **Intervalos de monitor > Medición de ruido**, y el rango permitido es de 60 a 3600 segundos. Si se deja en el valor predeterminado de 180 segundos, los AP escanean cada canal en el grupo de canales una vez, durante 50 ms, cada 180 segundos. Durante este período, la radio AP cambia de su canal de servicio al canal especificado, escucha y registra valores durante un período de 50 ms y luego vuelve al canal original. El tiempo de salto más el tiempo de permanencia de 50 ms lleva el AP fuera del canal durante aproximadamente 60 ms cada vez. Esto significa que cada AP gasta

aproximadamente 840 ms del total de 180 segundos escuchando a los rogues.El tiempo de "escucha" o "permanencia" no se puede modificar y no se cambia con un ajuste del valor de Medición del ruido. Si se reduce el temporizador de medición de ruido, es probable que el proceso de detección de ruido encuentre más sospechosos y los encuentre más rápidamente. Sin embargo, esta mejora se produce a expensas de la integridad de los datos y del servicio al cliente. Por otra parte, un valor más alto permite una mejor integridad de los datos, pero reduce la capacidad de encontrar a los piratas rápidamente.

5. Configure el modo de operación AP:Un modo ligero de operación AP define la función del AP. Los modos relacionados con la información presentada en este documento son:**Local**: es la operación normal de un AP. Este modo permite que los clientes de datos sean atendidos mientras se escanean los canales configurados para detectar ruido y rogues. En este modo de funcionamiento, el AP se apaga del canal por 50 ms y escucha a los rogues. Se desplaza a través de cada canal, de uno en uno, durante el período especificado en la configuración de RF automática.**Monitor**: es el modo de radio receive only y permite que el AP escanee todos los canales configurados cada 12 segundos. Solamente los paquetes de desautenticación se envían en el aire con un AP configurado de esta manera. Un AP de modo monitor puede detectar rogues, pero no puede conectarse a un rogue sospechoso como cliente para enviar los paquetes RLDP.**Nota:** DCA se refiere a los canales no solapados que se pueden configurar con los modos predeterminados.**Detector no autorizado**: en este modo, la radio AP se apaga y el AP escucha sólo tráfico por cable. El controlador pasa los APs configurados como detectores rogue así como listas de clientes sospechosos rogue y direcciones MAC AP. El detector no autorizado escucha sólo los paquetes ARP y puede conectarse a todos los dominios de difusión a través de un link troncal si lo desea.Puede configurar un modo AP individual simplemente, una vez que el Lightweight AP está conectado al controlador. Para cambiar el modo AP, conéctese a la interfaz web del controlador y navegue a **Wireless**. Haga clic en **Detalles** junto al AP deseado para mostrar una pantalla similar a
esta:



Utilice el menú desplegable AP Mode para seleccionar el modo de funcionamiento AP deseado.

Comandos para resolución de problemas

También puede usar estos comandos para solucionar problemas en la configuración en el AP:

- **show rogue ap summary**: Este comando muestra la lista de AP rogue detectados por los AP ligeros.
- **show rogue ap detailed** *<dirección MAC del rogue ap>* —Utilice este comando para ver detalles sobre un AP rogue individual. Este es el comando que ayuda a determinar si el AP rogue está conectado a la red cableada.

Conclusión

La detección y la contención de elementos no deseados dentro de la solución de controlador centralizado de Cisco es el método más eficaz y menos intrusivo del sector. La flexibilidad proporcionada al administrador de la red permite un ajuste más personalizado que puede adaptarse a cualquier requisito de red.

Información Relacionada

- Descripción General de los Grupos de RF

- Soporte Técnico y Documentación - Cisco Systems